Identity Theft: The Name Game



 Identity Theft continues to be the fastest growing crime in the nation.

 Learn the basics- What it is, how it works, who the perpetrators are and how to defend against them.







 Most data compromise - <u>90 percent</u> takes place through traditional offline channels and not via the Internet.

Lost or stolen wallets, checkbooks or credit cards continue to be the primary source of personal information theft when the victim can identify the source of data compromise. (30 percent).

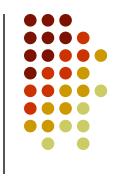
Identity Fraud Trends



3. Almost half (47 percent) of all identity theft is perpetrated by friends, neighbors, inhome employees, family members or relatives - someone known.

4. Nearly 70 percent of consumers are shredding documents, so that trash as a source of data compromise is now less than 1 percent.

Identity Fraud Trends



- 5. The 65+ demographic age group has the smallest rate of identity fraud victims (2.3%)
- 6. Over half the victims were 18-39 years old (29% for ages 18-29 The 35-44 demographic age group has the highest average fraud amount (\$9,435).



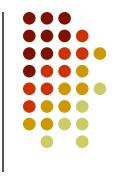


Low tech" Identity Criminals

 Dumpster Divers (commercial and residential trash)

Theft of wallets, purses, and mail

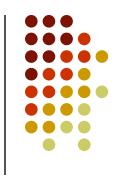




High Tech Identity Criminals

- Internet (company databases, websites)
- Public Domain public filings, like deeds and some court records).
- Collusive Employees
- Hacking
- Email and telephone scams (phishing & pretexting).
- Careless online shopping and banking

Main Types of Identity Theft



Financial ID Theft

Criminal ID Theft

Identity Cloning





The weapon? Personal information:

Name

Address

Mother's maiden name

Date and place of birth

Social Security number

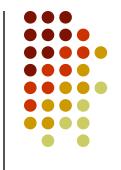
"Once they have this information, they own you.... They are you."

Financial ID Theft



- With "phishing" scams, criminals send out bogus e-mails telling recipients that they need to confirm certain account details to reactivate their accounts or claim prizes
- With "Skimming" a data storage device that captures credit card information
- NOTE: Legitimate businesses and organizations do not send emails or popups to request personal information.





 Telemarketers asking for personal information or using scare tactics to get it.

"Your insurance has lapsed and we need your personal information to reinstate it today."

"This is the IRS and we are having trouble depositing your economic stimulus check, we need your account number and

.

What Can Be Done with this Info?



- Apply for credit or loans
- Establish utility service
- Obtain a cell phone
- Obtain insurance
- Apply for a job

Criminal ID Theft



 The imposter in this crime provides the victim's information instead of his or her own when stopped by law enforcement. Eventually when the warrant for arrest is issued it is in the name of the person issued the citation- yours.

Identity Cloning



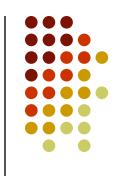
- In this crime the imposter uses the victim's information to establish a new life. They work and live as you.
- Examples: Illegal aliens, criminals avoiding warrants, people hiding from abusive situations or becoming a "new person" to leave behind a poor work and financial history.

STAY ALERT (WARNING SIGNS)



- Failing to receive bills or other mail.
- Receiving credit cards that you didn't apply for.
- Being denied credit, or being offered less favorable credit terms, like a high interest rate, for no apparent reason.
- Getting calls or letters from debt collectors or businesses about merchandise or services you didn't buy.

What Should I Do To Avoid Becoming A Victim



 To reduce or minimize the risk of becoming a victim of identity theft or fraud, the Identity Theft Resource Center recommends. For starters, just remember the word "SCAM":

Avoid Becoming a Victim



S - Be stingy with your personal information – don't give it to others unless you have a reason to trust them, regardless of where you are.

Avoid Becoming a Victim



C - Check your financial information regularly, and look for what should be there and what shouldn't. You generally have 60 days to dispute items on your bank statement.





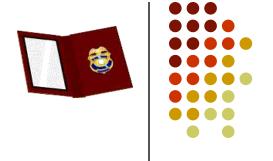
A - Ask periodically for a copy of your credit report. (Online at www.annualcreditreport.com, or call 1–877–322–8228, or TDD at 1–877–730–4104.)





M - Manage and maintain your personal information in a safe place.

What Should I Do If I've Become A Victim



Get an ID Theft Victims Kit.

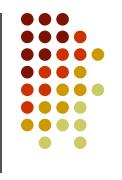
- Report the incident to law enforcement. (Your local police department or the Kentucky State Police.)
- ☑ Call the fraud units of the three main credit bureaus and ask that your credit reports be "flagged with a fraud alert".

What Should I Do If I've Become A Victim



- Consider putting a "security freeze" on your credit report with each credit bureau.
- Opt out of receiving pre-screened or pre-approved credit offers.
- When ordering your free annual credit report, go to <u>annualcreditreport.com</u>.

Identity Theft



 No matter what type of identity theft is involved. The result is a long and sometimes arduous road to recover.

 As in all crimes, preventing the crime from occurring in the first place is key.

Identity Theft is a Crime



QUESTIONS?